**University of South Carolina**
**Department of Computer Science and Engineering**

# Seminar Announcement

**Date**: March 29, 2004
2:00-4:00 pm
**Location**: USC, Law School Auditorium

# DOMESTIC AND INTERNATIONAL ASPECTS OF HOMELAND SECURITY LAW

**Bret Michael**
Dept. of Computer Science
Naval Postgraduate School
*Monterey, Calif. 93943*

***Tom Wingfield***
*The Potomac Institute for Policy Studies*
*Arlington, Va. 22203*

**Abstract**

The law governing cyber intrusions is inextricably bound to the technology for implementing it. Recent advances in the development of decoys, honeypots, and related concepts have raised a host of legal issues, but have also provided new opportunities for technologists and lawyers, working together, to expand the breadth and effectiveness of defensive actions. The law, while complex in detail, is based on general principles which should be familiar to technologists responsible for protecting systems of critical importance.

One such concept is that of categorical legal identity—the minimum identification necessary to react to an intruder with the widest possible range of lawful options. Evidence gathering, intelligence collection, or military hack-back are each conducted under their own legal regimes, and choosing the proper one is the first task of the cyber lawyer. An intruder's true identity may never be known, but his categorical legal identity—the minimum information necessary to treat him as a terrorist, or a criminal, or a soldier, or a spy, or a script kiddy—may be defined in advance and uncovered rapidly in the course of an intrusion. This will allow for an immediate, appropriate, and lawful response.

Distinguishing "uses of force" under international law from other activities (employing the Schmitt analysis), following the four fundamental legal principles of armed conflict (in the cyber or kinetic world) of cyberspace, and designing response systems which optimize the human and cyber elements of a system (ala THEMIS) are immediate priorities for academics and practitioners.

**For further information contact:**
Csilla Farkas
Dept. of Computer Science and Engineering
farkas@cse.sc.edu
www.cse.sc.edu/~farkas
576-5762

**THOMAS C. WINGFIELD**

National security attorney with extensive military and intelligence community experience, currently serving as Director of Tyranny, Democracy, and Regime Change at the Potomac Institute for Policy Studies. Provides legal and policy analysis to the federal national security community with a focus on international cyber law, protection of critical infrastructure, and the targeting of regime elites. Knowledge of Russian language, has served as an analyst within the intelligence community and as the Senior Military Social Aide for the White House. Author of legal text, *THE LAW OF INFORMATION CONFLICT: National Security Law in Cyberspace*. Lecturer in Law at Columbus School of Law, the Catholic University of America.

**EDUCATION**

S.J.D., (Candidate), National Security Law, University of Virginia Law School, *"Legal Bases for Effecting Regime Change in Democidal Tyrannies."*

1999 LL.M., *with distinction*, International and Comparative Law, Georgetown University Law Center,

1996 J.D., Georgetown University Law Center

1987 B.A., *summa cum laude*, *with distinction* in History, Georgia State University

**JAMES BRET MICHAEL**

Bret Michael conducts research, in collaboration with Tom Wingfield, for the Department of Homeland Security on the technical and legal aspects of cyberterrorism and lawful responses to it, in addition to developing course materials in support of the Naval Postgraduate School's Homeland Security Leadership program. He provides leadership as principal investigator for several large, multidisciplinary research projects sponsored by the Missile Defense Agency, National Security Agency, and other government agencies. He joined the Department of Computer Science at the Naval Postgraduate School in 1998 and was awarded tenure as Associate Professor in 2003. He has held research appointments with the University of California at Berkeley (1994-1998), Argonne National Laboratory (1992-1993), and the Institute for Defense Analyses (1988-1992). He was elected in 1997 to the grade of senior member of the Institute of Electrical and Electronics Engineers (IEEE) in recognition of his research on automated vehicle control and safety systems. He serves on several advisory boards and steering committees for the U.S. Government, editorial boards for the Journal of Information and Management (North-Holland) and IEEE Software, as the Chair of the Technical Committee on Assurance for the IEEE Reliability Society, and as an Adjunct scientist with the Office of Naval Research International Field Office (London) to foster collaboration between the Department of the Navy and the Russian Academy of Sciences.

**EDUCATION**

2004 Certificate, National Security Law, National Security Law Institute, University of Virginia, Charlottesville, Va.

1993 Ph.D., Information Technology, George Mason University, Fairfax, Va.
Dissertation: A Formal Process for Testing the Consistency of Composed Security Policy

1987 M.S., Information Systems, George Mason University, Fairfax, Va.

1985 M.B.A., (specialization in accounting theory), George Mason University, Fairfax, Va.

1983 B.S., Business Administration (minor in Mathematics), West Virginia University, Morgantown, W.Va.

**USC-GMU-NPS-POTOMAC INST.**
**JOINT RESEARCH ON LAWFUL CYBER SECURITY RESPONSE**

# THEMIS: Threat Evaluation Metamodel for Information Systems Legislation, Response, Ontologies, and Rules

C. Farkas[1], T. C. Wingfield[2], J. B. Michael[3] and D. Wijesekera[4]
[1]Dept. of Computer Science and Engineering, USC, Columbia, S.C. 29208
[2]The Potomac Institute for Policy Studies, Arlington, Va. 22203
[3]Dept. of Computer Science, Naval Postgraduate School,
Monterey, Calif. 93943
[4]Dept. of Information and Software Engineering, GMU, Fairfax Va. 22030

THEMIS: **Th**reat **E**valuation **M**etamodel for **I**nformation **S**ystems is a Description Logic based framework to apply national and international law to computer network attacks. It can be useful for law enforcement agencies and prosecutors building legally sound arguments, and for network designers to keep their retaliatory measures within legal limits. To do so, THEMIS automates know quantitative measures of characterizing attacks and their potential impact to place them in appropriate legal compartments. From the perspective of computer networks, we develop representations of cascading attack consequences to reason about complex attacks that are made of atomic actions. From the perspective of law, we propose the development of interoperable rules representing legal restrictions over heterogeneous domains. The two threats are weaved together in THEMIS in a form of description logic to reason about and guide prosecutory and retaliatory actions. Our model uses emerging Semantic Web standards, like Web Ontology Language (OWL), Rule Markup Language (RuleML), and Semantic Web Rule Language (SWRL). This paper shows the current state of our work and demonstrates the applicability of the proposed framework via an example of Schmitt Analysis - used to quantify whether a computer network attack represents armed coercion according to international law and, thus justify armed retaliation.

Accepted for *2nd Symposium on Intelligence and Security Informatics*, June 10-11, 2004, Tucson, AZ

**CSILLA FARKAS**
Csilla Farkas is an Assistant Professor in the Department of Computer Science and Engineering and Director of the Information Security Laboratory at the University of South Carolina. Csilla Farkas received her Ph.D. from George Mason University, Fairfax. In her dissertation she studied the inference and aggregation problems in multilevel secure relational databases. Her current research interests include information assurance, data inference problem, national and international law for cyber security, and Secure Semantic Web. Dr. Farkas is a recipient of the National Science Foundation Career award. The topic of her award is "Semantic Web: Interoperation vs. Security - A New Paradigm of Confidentiality Threats".

**DUMINDA WIJESKERA**
Duminda Wijesekera is an Assistant Professor in the Department of Information and Software Engineering at George Mason University, Fairfax, Virginia. His current research is in information, network and telecommunication security. Previously, he served as a senior systems engineer at Honeywell Space Systems, an assistant professor of mathematics at the University of Wisconsin, and a visiting post-doctoral fellow at the Army High Performance Research Center of the University of Minnesota. Dr. Wijesekera received a Ph.D. in Computer Science from the University of Minnesota and a Ph.D. in Mathematical Logic from Cornell University. In the past, he has worked in avionics control, quality of service, multimedia systems and program verification.